Federal PKI CONOPS

Bill Burr
National Institute of Standards and Technology
301-975-2914
william.burr@nist.gov
September 10, 1998
TWG-98-61

CONOPS History

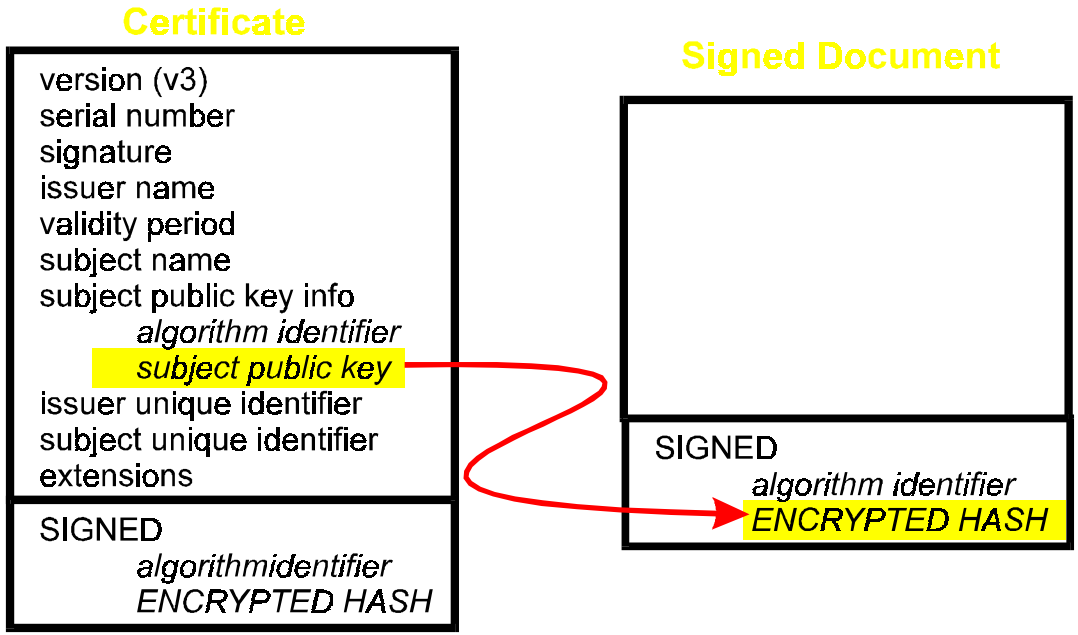
- First Draft in 1994
  - by Feb. ‘96 in it’s 14th revision
  - Now in it’s 20th revision.
- Intended as a part of a set
  - certificate and CRL profile
  - FPKI requirements
  - Technical security policy document
  - CONOPS

CONOPS Purpose

- Define the overall *technical* approach to the Federal PKI
  - capture the conclusions of the TWG
  - define a certification path architecture
- An introduction to PKI technology for intelligent and interested readers
  - tutorial material

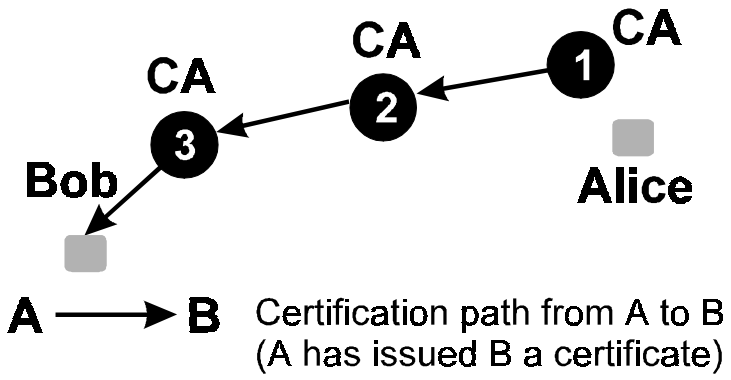
X.509 Based from the start

- Uses X.509 certificates
  - no alternative ever seriously considered

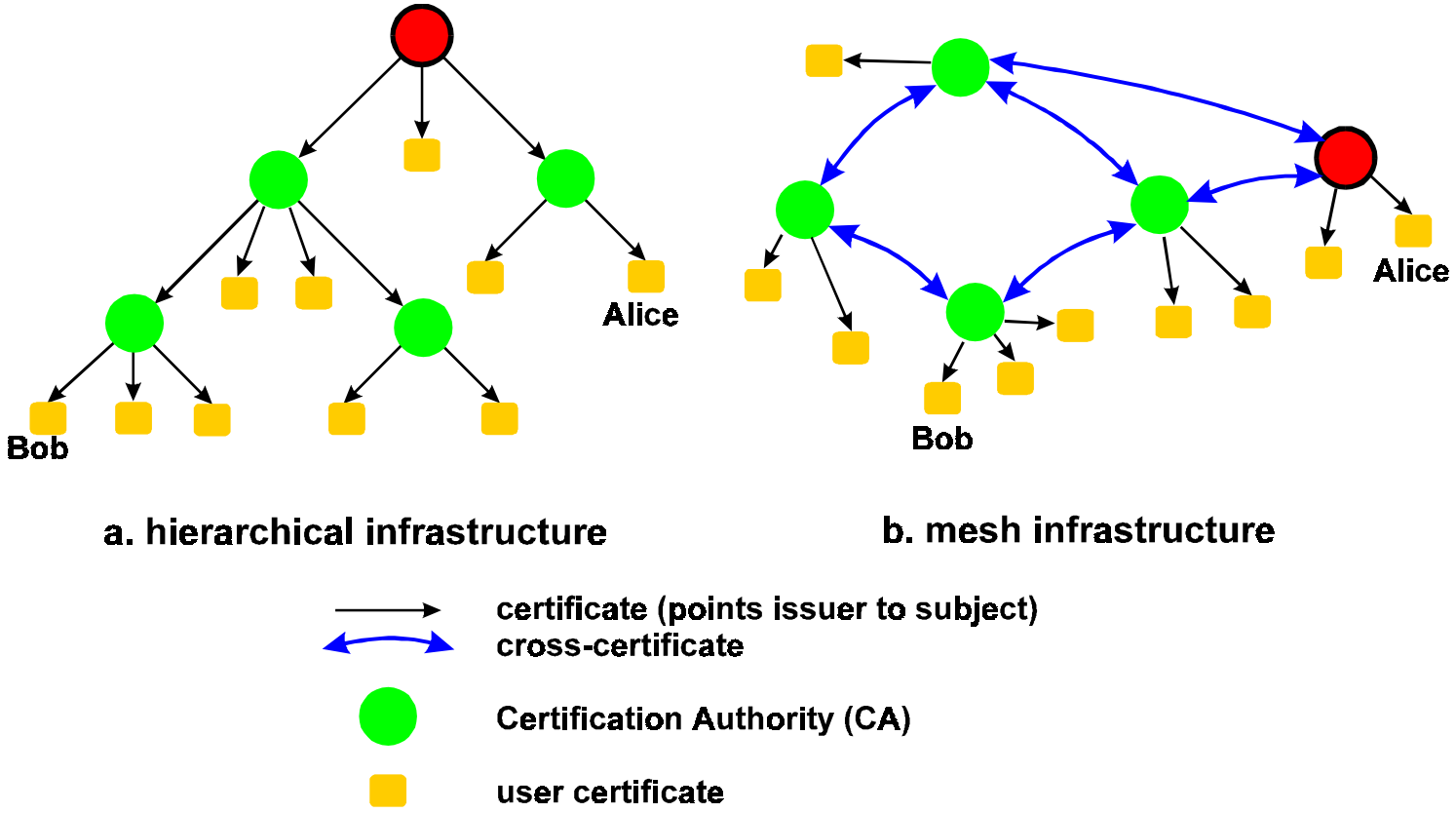


Certification Path

- Alice can verify Bob's certificate by verifying a chain of certificates ending in one issued by a Certification Authority (CA) she trusts (and whose public key she knows)

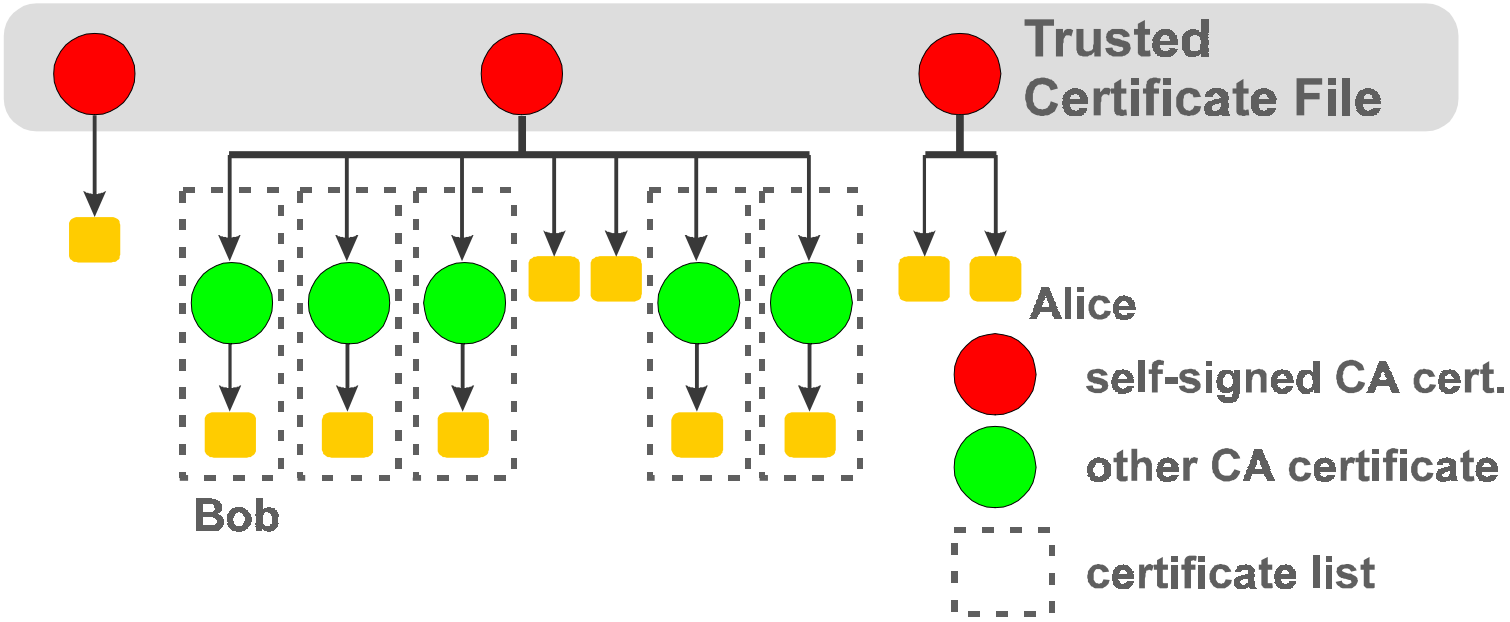


Hierarchy or Mesh



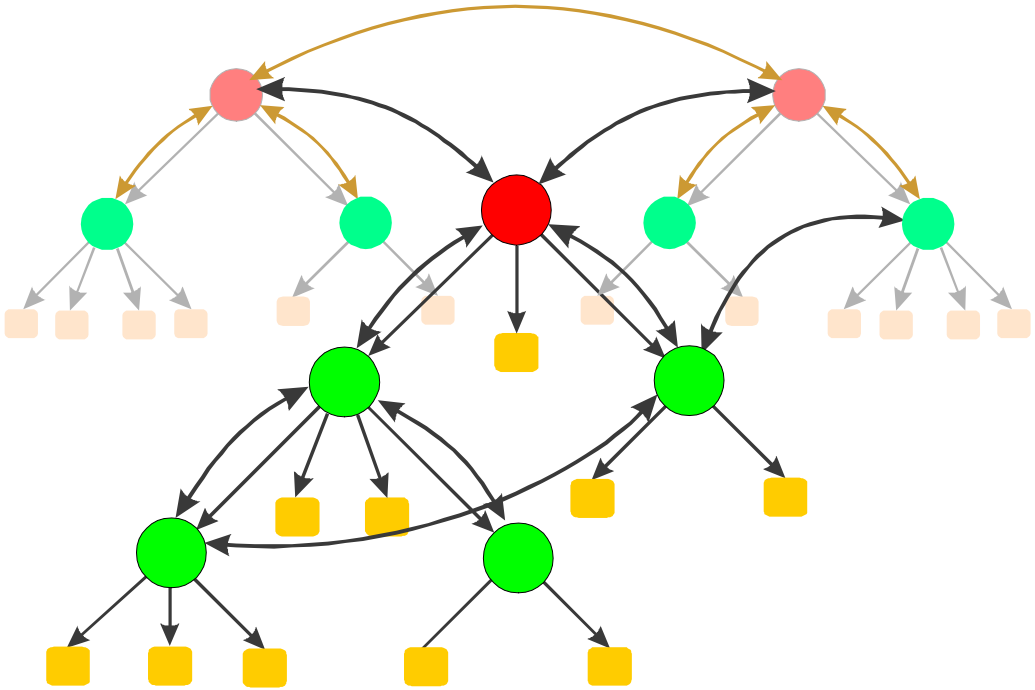
Trust-List Oriented PKI

- Predominates in WWW apps. today



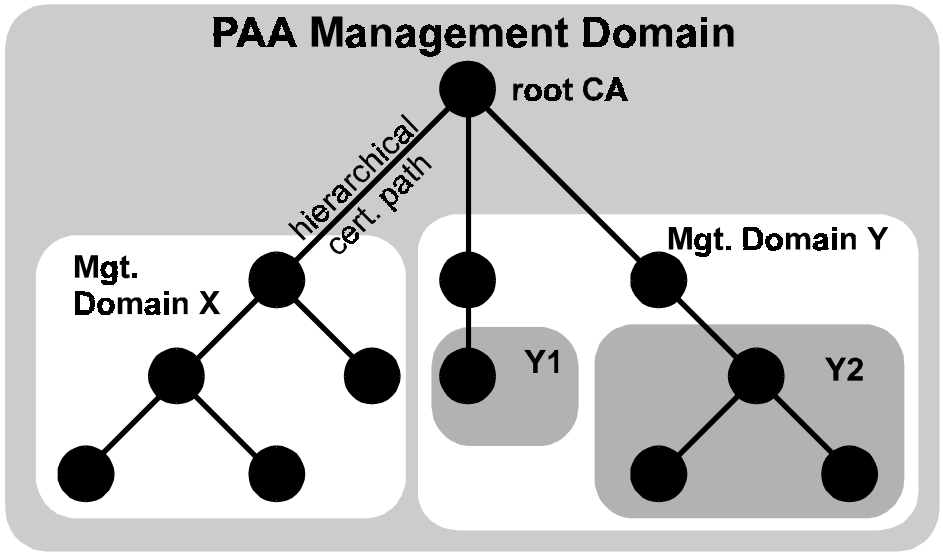
Old CONOPS Architecture

- Hybrid, with strong hierarchical flavor



Old PKI Policy Management

- Old approach hierarchical
  - technical controls in certification path



Old Algorithm & Interoperability

- Agencies Limited to DSS by FIPS
  - waivers needed for RSA
- No key management algorithm FIPS
- “End-Systems” approach to interoperability
  - end systems should be able to verify signatures for all common algorithms

Current Situation

- Numerous Federal PKI pilots
  - built and paid for for some agency application
    - » justified in terms of benefit to that application
  - no other vehicle for funding
- Different Architectures
  - mesh (many Entrust-based pilots)
  - Trust-List (ACES)
  - Hierarchical (MISSI-DMS, DoD medium)

Current Situation

- Many different pilots that use certificates, but
- Little interoperability between them
- Has been more difficult than you would think even to achieve cert. path interoperation between CAs from the same vendor.

Current Situation

- No will or funding to build the management apparatus to impose strong hierarchical policy management
- Agencies value their independence and have different missions and needs

Current CONOPS Approach

- Build on what is happening anyhow
- Supply the nexus to connect the pieces
  - Three key elements:
    - » Federal Policy Management Authority (PMA)
    - » Federal “Bridge” CA (BCA)
      - not a root
      - cross certifies with CAs
    - » Bridge CA Repository
      - for CA certificates and status

Federal PMA

- Overall management of FPKI
- Supervises BCA and BCA Repository
- Sets overall Federal Certificate Policies
  - assurance levels
  - model policies
- Approves Bridge CA cross-certification
  - reviews CA CPS

Trust Domain

- A group of CAs that
  - operate under the supervision of a Domain Policy Management Authority
  - use consistent policies, and have similar Certification Practice Statements (CPS)

Bridge CA (BCA)

- Cross certifies with “Principal CA (PCA)” in each trust domain
  - ***not a root***: does not start cert paths
  - may have constraints in the certs it issues
  - also cross certifies with non-Federal PCAs
- Issues consolidated Authority CRL (ARL)
  - CRL for all Federal CAs (and perhaps others)
  - Modest size, since CA certs. are not volatile

Bridge CA Repository

- One-stop shopping for CA certificates
  - CA certs. for the Federal PKI
  - ARL
- High availability
  - key to building cert. paths
- Medium bandwidth
  - everything it holds can be cached
  - ARL should not be large

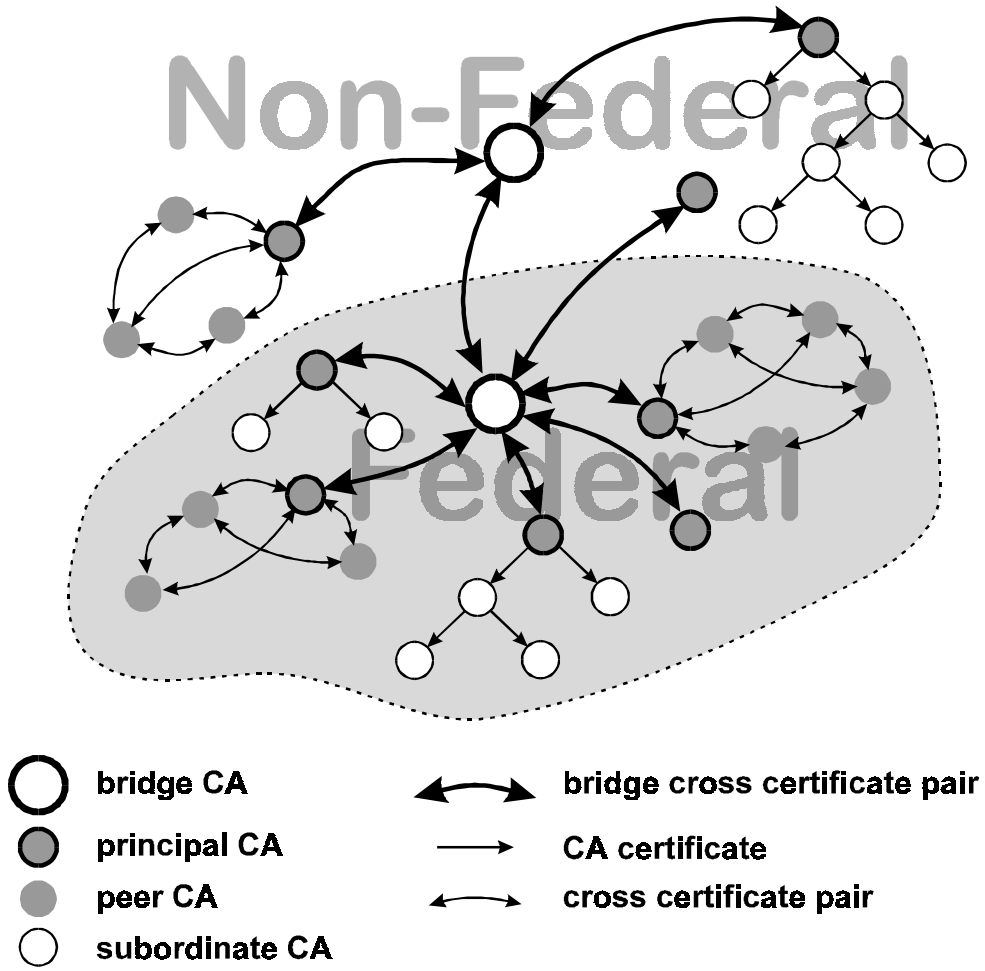
BCA OCSP Responder?

- Possibility, if OCSP catches on
- Would provide on-line equivalent to ARL

Principal CA

- Designated CA in each trust domain
- Has cert. path to all other CAs in the domain
- In hierarchical domain, the root CA

CONOPS FPKI Architecture



Carrots, not Sticks

- Participation should be voluntary
  - no requirement for CAs to join
- Provides a way to connect local trust to a wider Federal PKI
  - a form of recognition
  - avoid the cost and management headache of managing many cross-certifications
  - acceptance of PMA policy management

Changes

- Much editing
  - ran through WORD grammar checker (UGH)
  - many editorial comments
- New material
  - Bridge CA Concept
  - more on attribute certificates

Changes

- Bridge CA concept incorporated (June draft)
  - PMA, much less authoritarian style of management
  - Bridge CA does not start Cert paths and cross certifies with CAs who meet PMA's rules
  - Wording from Guida Notional BCA paper (Sept. draft)

Changes

- Algorithm Interoperability
  - Accomplished between BCA and PCAs
    - » PCAs and trust domains generally use one algorithm
  - expect most common algorithms to be FIPS approved
  - still use “end-systems” approach
  - terminology revised
  - details of where mixed algorithm certs used not yet decided

Changes

- Policy & PMA (replaces PAA)
  - less hierarchical and authoritarian
  - aligned with Canadian Assurance level Policies
    - » 4 levels accepted
    - » ordered levels of assurance
    - » populate lower assurance levels in certificate
      - e.g., *rudimentary*, or *rudimentary* plus *basic*, or *rudimentary* plus *basic* plus *medium*
  - text extensively rewritten

CONOPS Issues

- Repositories
  - X.500/LDAP Directories vs alternatives
    - » Are there any alternatives?
    - » Directory Schema
      - granularity
      - cACertificate vs crossCertificatePair
      - border directories
      - referral vs shadowing

CONOPS Issues

- Detailed mixed-algorithm BCA certification path approach
- ACES
  - how does it fit in the FPKI?
    - » does the FPKI really reach the public at large?
- Cross-certification
  - what are the rules?
  - directory attributes

CONOPS Issues

- Revocation
  - what is the role of OCSP?
    - » some user interest
    - » vendor hostility
  - indirect CRLs
    - » ARL
  - use of distribution points